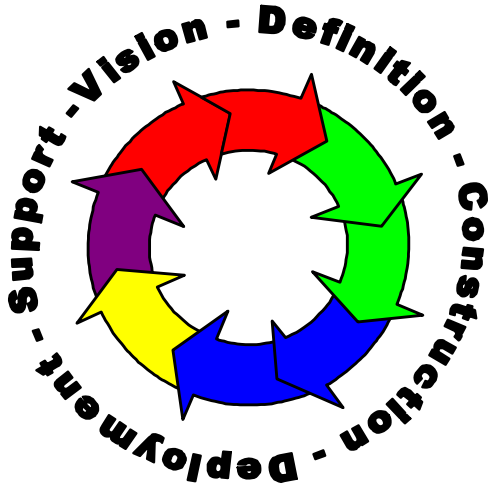


~~Student Financial Assistance~~Federal Student Aid

System Security Process Guide

~~September 25, 2001~~April 1, 2002

Table Of Contents

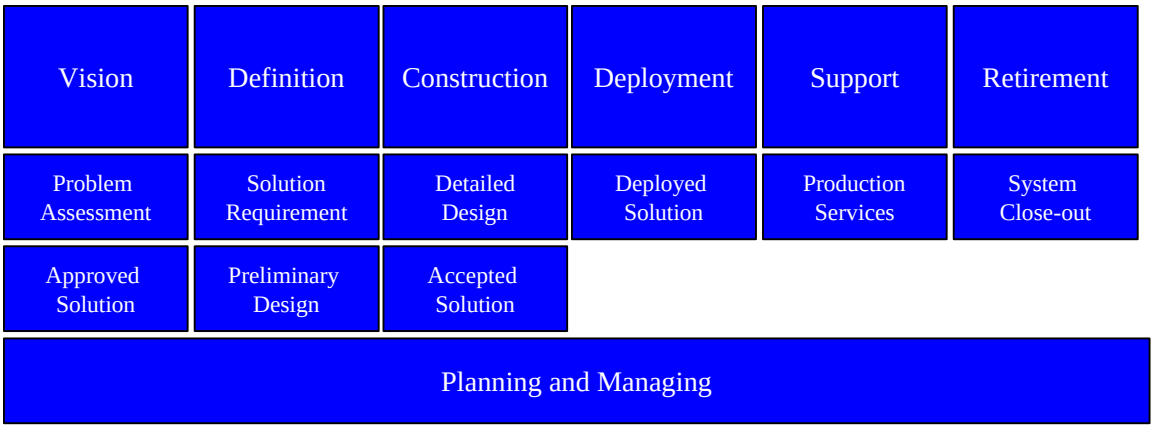
1.0 Introduction

As part of its commitment to customers and partners, ~~SFA~~FSA manages risks on a continuous basis. Faced with a public and administration that has a heightened awareness of security concerns, ~~SFA~~FSA needs to demonstrate that its systems are worthy of trust and consistent with best security practices and U.S. Public Law and policy. Security incidents could undermine the credibility of ~~SFA~~FSA, and greatly affect its ability to help put America through school. In addition to losing credibility, actual fraud and abuse could occur without adequate security and privacy controls.

The purpose of the system security process guide is to ensure that security is an integral component of all ~~SFA~~FSA systems. The guide includes numerous aides to assist the project team develop the security artifacts that will support the system's overall security posture and auditability. As the system progresses through the lifecycle, the project team will produce documents such as a system security plan and, for certification and accreditation, a system security authorization agreement. The guide also provides direction for security training requirements, continuity of operations plans,

Security is an integral component throughout the SLC. The following sections and appendices describe system security in sufficient detail to allow a project team to confidently implement security into their system (See appendix D for a detailed Security SLC Project Plan). For additional security-related information, ~~SFA~~FSA maintains a Security Reference Guide on its intranet. This site will be continually updated with the most recent security documents, artifacts, and guidance.

The diagram below highlights the security artifacts to be completed during the system's lifecycle and where the system acquisition planning activities are performed in the SLC.



- Business Case
- RFP Security Requirements
- Task Order Security Components
- List of Business Partners
- Assignments Letters
- Security Artifact File System
- Electronic Security Artifact File System

- System Roles and Responsibilities

~~? System Identification and Analysis~~

~~? Threat and Vulnerability Guidance~~

- ~~Security Guidance Compliance Matrix~~
- GSS/MA Inventory Form
- Interconnected System'(s) Security Documentation
- MOU/SLA
- C&A Project Plan
- System Rules of Behavior
- Constructed Clearance Requirement Matrix
- Approved Contractor Access Request Form

- Draft System Security Plan
- Draft COOP
- Draft DRP
- Draft SSAA

~~? Threat Analysis~~

- ~~Impact Analysis~~
- Risk Assessment Report
- Risk Assessment CAP
- Cost Benefit Analysis
- Final MOU/SLA
- Completed User Background Investigation Clearance Form
- Approved User Access Request Form
- System Access Letters to Contractor

- Completed CAP
- Security Test Plan
- Test Results
- Final SSAA
- Certification Letter
- Signed Accreditation Letter
- Final System Security Plan
- Final COOP
- Final DRP
- User Training Schedule
- Approved User Access Request Forms

- Re-Certified and Accredited SSAA
- Documented Completion of Test Results
- Updated Operational Procedures
- Updated Testing Results

- System Retirement Complete

2.0 Vision Phase System Security

The Vision Phase initiates the concept of the system. During this initial phase, security should already be considered while the system's business case and requirements are developed. During the vision phase, personnel with security responsibilities should be identified. Early identification of these personnel will promote the addition of security into the system's development from the initial concept and throughout its development. Moreover, the certification and accreditation (C&A) requirement for each system stresses the appointment of key personnel to manage the C&A process. Initially, the functional manager should assign, in writing, a system manager. The system manager, in turn, should assign, again in writing, a system security officer (See appendix C for example assignment letters). These two positions are usually Department of Education staff and are critical to the continual inclusion of security into the system. Care should be taken when considering who should be assigned the responsibility of System Security Officer, as that person will be the primary point of contact for all security related matters for the system (See appendix A for a description of the qualities and responsibilities of an SSO).

Primarily, the System Security Officer (SSO) should ensure the business case includes the necessary resources for adequately securing the system. Similarly, the RFP should include security requirements and evaluation and test procedures. The RFP should contain language to permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

The Task Order should contain numerous security components. Ideally, the task order should recognize the following security areas:

- Security Plan
- Risk Assessment
- Certification and Accreditation
- Disaster Recovery Plan
- Federal Policy and Regulations
- Departmental Policy and Regulations
- Controls for Personnel Security
- Configuration Management

If the system will interface or rely on any external system, Memoranda of Understanding and Service Level Agreements should be developed as the system progresses through the lifecycle. The first step is to identify and document a list of potential business partners. During the vision phase, a dialogue should be established with potential business partners to begin to address the future relationships the parties will maintain throughout the system's lifecycle.

The SSO should establish an appropriate filing system to adequately maintain, update, protect and distribute system documentation. To maintain all relevant system artifacts, the SSO should maintain two filing systems: paper based and electronic. The SSO should manage version control of all security documentation and track the distribution of security artifact copies.

Once all security tasks are completed and documented, the SSO should submit a vision phase checklist to the System Manager for signature. The checklist should identify all security accomplishments attained

during the vision phase as well the date of completion (See appendix B for sample checklist). The following table contains the security products that should be created during the vision phase. Several of these products are not created entirely for the security of the system, but merely contain security-related information.

- Business Case
- RFP Security Requirements
- Task Order Security Components
- List of Business Partners
- Assignment Letters
- Security Artifact File System
- Electronic Security Artifact File System

.

3.0 Definition Phase System Security

As the system progresses through the definition phase, several security actions should occur. The system should be defined as a new system or major modification to an existing system, and then further defined as a General Support System (GSS), a Major Application (MA), or an Application (A). If the system is determined to be an Application, the security documentation requirements are considerably less than for an MA or GSS. For example, security plans and risk assessments are not required, but are still recommended.

To determine the system's sensitivity and criticality, the SSO should support the completion of the GSS/MA Inventory worksheet. The system's sensitivity should be classified and the system's criticality should be defined. To define sensitivity, the system owner (and its data) should review the importance of confidentiality, integrity, and availability. These factors dictate the security controls necessary to protect the assets of the system. ~~Similarly, a security review should occur which will identify threats to the system as well as intrinsic vulnerabilities.~~ Once the system has been classified, several data analyses should be conducted to determine appropriate security controls. Initially, a system of record analysis should be performed to ascertain whether there are Privacy Act implications resulting from the system's data. If the system will contain Privacy Act data that requires system of record notification, a system of record schedule should be created and followed to ensure are federally imposed deadlines are met. Finally, the system's controls should be reviewed for federal and departmental policy compliance. At a minimum, the system should be reviewed for compliance with OMB Memorandum A-130 Appendix III, ~~the Privacy Act~~, GISRA (NIST Self-Assessment), Department of Education Policy, and ~~SFA~~FSA policy. ~~A security guidance compliance matrix should be constructed to document the findings of the review.~~

The System Manager should identify the roles and responsibilities of the user and developer community, to include ~~SFA~~FSA employees ~~(See appendix A for SSO Roles and Responsibilities)~~. During the definition phase, this community should be formally identified and their contact information should be documented.

If the system will be connected to another information source, the security documentation from the interconnected system should be obtained and reviewed. Likewise, the MOU/SLA agreements with the business partners and/or system owners should be drafted. The SSO should ensure security control input is included in the MOU/SLA.

During the definition phase, the SSO should undergo appropriate training to prepare for the responsibilities of an SSO during the life of the system. The Department of Education maintains online training curricula and there are also numerous training programs outside the department that may be appropriate for an SSO.

A key security component occurring during a system's development, the certification and accreditation process, begins in the definition phase. Initially, the project team guided by the SSO should develop the C&A project plan. This plan will provide a schedule and list of activities to be completed prior to the system's deployment. Several of the initial tasks are listed below.

- Identify responsible organizations/individuals
- Identify resources and funding

- Define system boundaries
- Create C&A schedule
- Register C&A with Agency Security Office

Several personnel security activities occur during the definition phase. The system rules of behavior should be developed using guidance found in NIST Special Publication 800-18 Appendix B. ~~Also, the privacy act should be taken into consideration to ensure compliance with federal privacy guidance.~~ The rules of behavior document informs the user of permissible actions while using the system and indicates the consequences of violating the rules of behavior policy. The contractor personnel should request access to the system by completing a rules of behavior form and returning the signed document to the SSO. This activity should be completed prior to granting access to the system.

Both ~~SFA~~FSA employees and contract support personnel should have some level of background screening prior to accessing the system. Specific clearance requirements should be developed for both ~~SFA~~FSA employees and contractors. The SSO should distribute background investigation clearance forms to the contract support personnel who will define and develop the system. After completing the required background screening, the contractor personnel should return the form to the SSO.

Once all security tasks are completed and documented, the SSO should submit a definition phase checklist to the System Manager for signature. The checklist should identify all security accomplishments attained during the definition phase as well the date of completion (See appendix B for sample checklist). The following table contains the security products that should be created during the definition phase. Several of these products are not created entirely for the security of the system, but merely contain security-related information.

- System Roles and Responsibilities

~~? System Identification and Analysis~~

~~? Threat and Vulnerability Assessment~~

- ~~Security Guidance Compliance Matrix~~
- GSS/MA Inventory Worksheet
- Interconnected System'(s) Security Documentation
- MOU/SLA Draft
- C&A Project Plan
- System Rules of Behavior
- Constructed Clearance Requirement Matrix
- Approved Contractor Access Request Form

4.0 Construction Phase System Security

The construction phase contains numerous security activities. A large portion of these activities is dedicated to documentation. Primarily, the system security plan should be drafted during this phase. To accomplish this task, the project team members should first organize the following security-related documentation:

- Architecture Diagram and/or design diagram
- Security Requirements
- Interfaces and connectivity
- Operating environment
- User role descriptions
- Description of data
- Process map

Guidance for completing the security plan can be found in NIST Special Publication 800-18. This reference document includes definitions, templates, and general guidance for creating a federally approved system security plan. Also during the construction phase, the continuity of operations and disaster recovery plan should be drafted. These plans describe how the system will continue its operation during an emergency situation.

In the construction phase, the certification and accreditation process directs the project team to draft a System Security Authorization Agreement (SSAA). The SSAA contains all certification documentation and is eventually presented to the Designated Approving Authority (DAA) for accreditation. To draft this document, the project team should first gather all essential information from the system security plan, COOP, DRP, etc. In essence, the SSAA is a central repository of system information contained in one, extensive document.

A risk assessment, conforming to the FSA Risk Assessment Guide, should be performed to determine if intended security controls are adequate to protect the system. ~~Using the sensitivity and criticality assessment completed in the definition phase, a threat analysis should be performed. The threat analysis consists of a control review and a likelihood determination. An impact analysis should then be conducted to determine the mission impact from the results of the threat assessment. By combining the threat analysis and impact analysis, a level of risk determination is made. A corrective action should be developed from the risk assessment findings. Prior to the CAP being implemented, management should perform a cost/benefit analysis to determine which security controls should be corrected.~~ The first step is to identify potential system vulnerabilities using physical and network tests, documentation reviews, and federal policy compliance reviews. A threat source should be associated with each vulnerability once the list is established. Each vulnerability/threat pair should be evaluated for its potential impact to FSA if exploited, and for the likelihood the vulnerability/threat pair could be exploited. The result of this analysis yields a level of risk determination. These findings should be documented in a Risk Assessment Report.

A corrective action plan (CAP) should be developed responding to each risk assessment finding. From the CAP, a Cost Benefit Analysis (CBA) should be conducted to determine which corrective action(s) should be implemented based on the costs to implement the proposed security controls versus the

security benefits received. Potentially, a particular security control is cost prohibitive and therefore should not be implemented. ~~Rather~~In this instance, management should formally accept the residual risk.

During the construction phase, the SSO should obtain and review the MOU/SLA for inclusion of appropriate security controls. If necessary, the SSO should make and submit additional security control inputs to the business partners and/or system owners.

Background investigations should be completed for all users of the system, as was completed for contract support personnel in the Definition phase. The SSO should issue requests for user background investigations per ~~SFA~~FSA requirements. Once completed, the SSO should collect completed contractor background investigations and maintain the file. Also, users of the system and contract support personnel should complete user access forms and sign a system rules of behavior document. The SSO should distribute the two forms to the user community and, once completed, collect the forms. The forms should be maintained for the life of the system.

Once all security tasks are completed and documented, the SSO should submit a construction phase checklist to the System Manager for signature. The checklist should identify all security accomplishments attained during the construction phase as well the date of completion (See appendix B for sample checklist). The following table contains the security products that should be created during the construction phase. Several of these products are not created entirely for the security of the system, but merely contain security-related information.

- Draft System Security Plan
- Draft Continuity of Operation Plan
- Draft Disaster Recovery Plan
- Draft System Security Authorization Agreement

~~? Threat Analysis~~

- ~~Impact Analysis~~
- Risk Assessment Report
- Risk Assessment Corrective Action Plan
- Cost Benefit Analysis
- Final MOU/SLA
- Completed User Background Investigation Clearance Form
- Approved User Access Request Form
- System Access Letters to Contractor Employees

5.0 Deployment Phase System Security

In the Deployment phase, several security related activities introduced in prior phases should be brought to closure. The corrective action plan developed in the construction phase risk assessment should be implemented. Once implemented, each CAP element should be dated and initialed indicating completion of the element. The CAP should then be submitted to the SSO for maintenance.

The construction phase reviewed the security controls as they are documented. During deployment, the security controls should undergo a series of tests to determine if the controls were implemented properly and effectively. Initially, a security test plan should be developed, including the following elements:

- Security Test and Evaluation
- Penetration Testing
- System Management Infrastructure Analysis
- Site Evaluation
- Contingency Plan Evaluation

The system's security controls, including those controls implemented as a result of the corrective action, should be tested and evaluated. All system security tests should be thoroughly documented and recorded in a formal test results document.

The Certification and Accreditation process should approach completion during the deployment phase. The SSAA drafted in the construction phase should be delivered to the System Manager (SM) for review. After reviewing the SSAA for content, quality, and degree of completion, the SM should make a recommendation to the Designated Approving Authority (DAA). The recommendation should be one of the following:~~,~~ full accreditation, Interim Approval to Operate, or Not to turn on. The SSAA should be presented to the DAA and executive level findings should be discussed. Finally, the SSO should attend the PRR as a security representative to respond to any concerns presented during the PRR. At the PRR, the DAA should sign the accreditation letter if appropriate. The SSO should obtain a copy of the signed accreditation letter and maintain a copy in the security file.

The System Security Plan begun in the Construction phase should be completed prior to the system becoming operational. Upon completion of the plan, the SSO has the option to submit the SSP to ~~SFA~~FSA/CIO Security Office for a NIST Special Publication 800-18 compliance review. The review will identify potential areas of improvement and recommend corrective actions. Two more plans should be finalized during this phase. The Continuity of Operation and Disaster Recovery plans should be completed and tested prior to the system becoming operational. These plans will provide detailed response procedures if a major disaster occurs or if the system goes offline unintentionally for any period of time.

The SSO should identify opportunities for training that will directly support the job's performance. A schedule of proposed training opportunities should be created to assist the SSO plan an appropriate training regimen.

User access forms should be distributed by the SSO to all personnel who need access to the system once it becomes live. Upon completion, the SSO should collect the access request forms and maintain the forms in the security file.

Once all security tasks are completed and documented, the SSO should submit a deployment phase checklist to the System Manager for signature. The checklist should identify all security accomplishments attained during the deployment phase as well the date of completion (See appendix B for sample checklist). The following table contains the security products that should be created during the deployment phase. Several of these products are not created entirely for the security of the system, but merely contain security-related information.

- Documented Completion of CAP from Construction Phase
- Security Test Plan
- Test Results
- Final SSAA
- Certification Letter
- Signed Accreditation Letter
- Final System Security Plan
- Final Continuity of Operation Plan
- Final Disaster Recovery Plan
- User Training Schedule
- Approved User Access Request Forms

6.0 Support Phase System Security

The support phase continues throughout the life of the system. Once the system is deployed, several security activities and documents should be completed or updated. The System Security Plan should be reviewed and updated as the system undergoes major changes; that is, undergoes changes significant enough to alter the security posture of the system. OMB Circular A-130 Appendix III requires a review of security controls every three years or upon major system change. ~~SFA~~FSA recommends these reviews occur every year due to the rate of system change occurring at ~~SFA~~FSA. Also, the Government Information Security Reform Act (GISRA) requires a program and system review every year. The guidance to be used for this review can be found in the NIST Self Assessment Guide for Information Technology Systems. The self-assessment review will assist the SSO and system owner determine security control priorities based on weaknesses in policy, procedures, implementation, testing, and integration.

The system should undergo a re-certification and accreditation every three years or upon major system change. This process should analyze any new functionality or configurations the system may have adopted as well as any associated security controls. The analysis should be documented in the SSAA, as it was in the previous phases.

While the system is in operation, the SSO is responsible for continuous personnel security maintenance. The SSO should review and authorize system access privileges on a per case basis, provide periodic review of user access privileges and delete user accounts as necessary. The SSO should identify potential new users, ensure clearance forms are completed by the new user(s), track the clearance process, and notify the user(s) when their clearance process has completed. The SSO should maintain a copy of the authorized access requests in the security file.

The SSO also is responsible for training requirements, namely rules of behavior and security awareness training. All new users should review, understand, and sign a rules of behavior form indicating their acknowledgment of acceptable system-related activities. Also, ~~SFA~~FSA policy directs all system users to undergo annual security awareness training. Along with the rules of behavior form, the SSO should direct all new users to receive security awareness training

The Risk Management cycle also continues in the support phase. The testing of security controls in the Deployment phase may have identified areas of improvement. The test results should be implemented expeditiously. As new controls are implemented, testing procedures should be performed to ensure the controls adequately protect the intended assets. Also, as new threats are discovered from sources such as audit logs, security alerts, etc., the system's security controls should be updated in response. The COOP and DRP should be tested annually, while incorporating any new operational procedures in the system security plan.

Once all security tasks are completed and documented, the SSO should submit a support phase checklist to the System Manager for signature. The checklist should identify all security accomplishments attained during the support phase as well the date of completion (See appendix B for sample checklist). The following table contains the security products that should be created during the support phase. Several of these products are not created entirely for the security of the system, but merely contain security-related information.

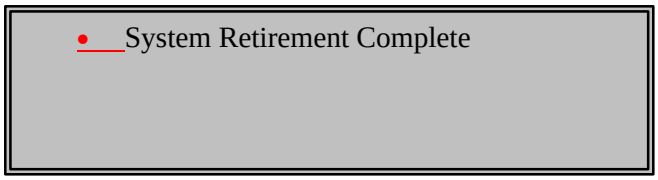
- Re-certified and Accredited SSAA
- Documented Completion of Test Results
- Updated Operational Procedures
- Updated Testing Results

7.0 Retirement Phase System Security

The purpose of the retirement phase is to ensure all sensitive data has been sanitized or destroyed once the system is no longer in service. The SSO should create an archive data retention matrix and destruction plan. This plan will guide the SSO and all associated personnel throughout the retirement phase. Any data to be reused should be archived in a useable format. Electronic records should be disposed/archived properly.

The physical destruction of all system material, data, etc. should be carefully managed. All electronic media should be sanitized (purged, overwritten, degaussed, or destroyed) when no longer needed. All printed paper products with sensitive information should be destroyed and all documents should be destroyed when all data is destroyed.

Once all security tasks are completed and documented, the SSO should submit a retirement phase checklist to the System Manager for signature. The checklist should identify all security accomplishments attained during the retirement phase as well the date of completion (See appendix B for sample checklist). The following table contains the security products that should be created during the retirement phase. Several of these products are not created entirely for the security of the system, but merely contain security-related information.



Appendix A – Qualities and Responsibilities of a System Security Officer

The System Manager should formally appoint the SSO in writing as the person responsible for the day-to-day security operations of that system. If the Executive Sponsor has not formally appointed the System Manager, the Executive Sponsor should assume the role of the System Manager for the purpose of appointing the SSO.

A SSO should have a general knowledge of systems and exhibit the following qualities:

- ❑ Be capable of identifying system vulnerabilities and risks, and be able to recommend solutions to mitigate those risks
- ❑ Be familiar with the system and the system's security software
- ❑ Be familiar with the security requirements in the SLC
- ❑ Be able to react appropriately to system threats and incidents, including enactment of the system's Disaster Recovery Plan
- ❑ Have a functional knowledge of the business process the system supports
- ❑ Be familiar with Departmental and Agency security policy for IT systems
- ❑ Be trustworthy

SSOs implement SFA's security policy for a specific information system and are responsible for the protection and privacy of information processed or stored in that system. To fulfill these responsibilities, an SSO:

- ❑ Serves as the primary point of contact for all IT security matters of concern to the AIS
- ❑ Coordinates with the System Manager to determine appropriate security requirements for the system
- ❑ Serves as the system's CCB security champion by recommending approval / disapproval for system changes based on the risk to the security and privacy of the system
- ❑ Schedules and participates in system risk assessments
- ❑ Develops a risk mitigation strategy
- ❑ Coordinates the creation of the system's Disaster Recovery Plan, Continuity of Operations Plan and Security Plan,
- ❑ Implements and updates the system's Disaster Recovery Plan, Continuity of Operations Plan and System Security Plan
- ❑ Coordinates certification and accreditation and advise System Manager for system certification
- ❑ Coordinates requests for access ensuring proper clearances are completed, roles match access, and access is terminated when no longer required.
- ❑ Implements training and awareness for users in security and privacy matters
- ❑ Performs other functions that may be required to ensure the integrity, confidentiality, and availability of the AIS

Additional duties and responsibilities for System Security Officers can be found the "SFA Security Guide", and the Department of Education's "Information Technology Security Policy".

~~**Appendix A - System Security Roles and Responsibilities**~~

~~**Appointing a System Security Officer (SSO)**~~

The System Manager should formally appoint the SSO in writing. If the Executive Sponsor has not formally appointed the System Manager, the Executive Sponsor should assume the role of the System Manager for the purpose of appointing the SSO.

A SSO should have a general knowledge of systems.

- ? They should be capable of identifying system vulnerabilities and risks; and be able to recommend solutions to mitigate those risks.
- ? They should have good judgment and have the ability to administratively track security matters to include providing and maintaining user accesses.
- ? They should have a functional knowledge of the system.
- ? They should also be knowledgeable on the security software the system uses and the SFA disaster recovery processes.

To assist the System Manger in SSO appointment, a list of duties relating to the SSO position can be found below. This list is a composite of Departmental documentation.

1. From the "Information Technology Security Policy":

A SSO is an individual formally designated by an IT system's business manager to be responsible for the day-to-day security operations of that system.

The primary function of a SSO is to implement the Department's ITSP as it applies to the system and the information that it handles or stores. The SSO shall work in close coordination with the CSO and the IT system business manager. Specific SSO duties include, but are not limited to —

- ? Implementing IT security for the assigned system.
- ? Serving as the primary point of contact for all IT security matters of concern to the AIS and be directly involved in configuration management processes and in the certification and accreditation process for their assigned system.
- ? Serving as liaison between the CSO and other personnel responsible for IT security activities, including the AIS business manager and any other owners of data, software, and hardware within the PO.
- ? Monitoring the implementation of the ITSP as it pertains to his or her AIS and, if significant deficiencies are disclosed, providing the evaluation results to the business and system managers as well as the CSO and the DCIO/IA. The information provided to the CSO shall include a plan of action for the correction of the deficiencies, including target completion dates.
- ? Ensuring implementation of security controls for the system, if deemed a critical IT infrastructure asset, through the execution of the CIP Plan.
- ? Maintaining contact with other security offices within the Department that focus on mission essential protection that are capable of providing indications and warnings for the Department's critical assets.
- ? Reporting IT security incidents to the appropriate CSO following the prescribed procedure for reporting and logging security incidents as described in the *Incident Handling Program Guide*.
- ? Overseeing risk assessments for his or her assigned AIS.
- ? Informing and overseeing operations personnel, as necessary, in the completion of all security functions.
- ? Reviewing and assuring the adequacy of the security plan developed by systems personnel.
- ? Participating in regular AIS security reviews.
- ? Developing AIS specific access authorization procedures.
- ? Performing other functions that may be required to ensure the integrity, confidentiality, and availability of the AIS.

2. From the "Certification and Accreditation Program Guide":

A System Security Officer (SSO) is an individual designated by the business manager of an IT system to be responsible for the day-to-day security of that system.

The primary function of an SSO is to implement the Department's ITSP as it applies to the system and the information that it processes or stores. The SSO shall work in close coordination with the CSO and the IT system business manager. Significant C&A responsibilities of the SSO include —

? Performing risk assessments for his or her assigned AIS
? Reviewing and assuring the adequacy of the security plan developed by systems personnel
? Participating in all AIS security reviews.

The SSO ensures that system security controls are designed, documented, tested, and implemented for his or her AIS. The SSO also ensures that the following actions that directly affect the C&A process take place —

? Addressing security in mission needs statement and all acquisition documents
? Incorporating security in all business and AIS functional and technical requirements
? Incorporating security architecture within system architecture (including hardware, software, firmware, and system interfaces)
? Addressing security in the configuration management (CM) plan
? Addressing security requirements in the system life cycle documentation
? Preparing security documentation
? Conducting security design and specification review
? Developing a contingency plan
? Performing security testing and reporting
? Performing operational testing and reporting.

3. From the "Security Awareness Training Program Guide":

System Security Officer (SSO)	Manages the day-to-day security operations for his or her assigned system. This includes the implementation of security awareness training. Receives guidance and direction from the CSO on security matters relevant to the assigned system.

4. From the "Risk Management Guide":

System Security Officer (SSO)	? Participates in assessing risk to his or her assigned AIS ? Documents the vulnerabilities identified in the AIS in the risk assessment report ? Reports to the CSO the vulnerabilities identified in the AIS ? Submits the risk assessment report and Risk Acceptance Recommendation to the CSO via the business or functional manager

5. From the "Security Incident Reporting Response Program Guide":

The System Security Officer's (SSO) incident handling duties include the following:

? Reporting IT security incidents to the appropriate CSO
? Performing corrective actions as directed in response to a reported incident.

The SSO is expected to know the following:

~~*? Department security policies for IT systems*~~
~~*? Common security threats*~~
~~*? Capability of recognizing system anomalies and assessing the impact of threats posed by those anomalies*~~
~~*? Methods used to recover from security breaches*~~
~~*? Methods used to prevent security breaches*~~
~~*? General technical knowledge of the system to coordinate responses to a security breach*~~
~~? Evidence of preservation techniques.~~

~~**6. From the "SFA Security Guide":**~~

~~**Coordinate** with SM to determine appropriate security requirements for system~~

~~**Inform** and **train** users in security and privacy matters~~

~~**Participate** in the system risk assessment (every three years) and develop a risk mitigation strategy~~

~~**Coordinate** requests for access with personnel clearance office~~

~~**Make sure** procedures for issuing and managing passwords are followed~~

~~**Recommend** approval / disapproval to the CCB for system changes based on the risk to the security and privacy of the system~~

~~**Develop** media marking, physical control, storage and disposal DRAFT requirements for assigned sensitive information~~

~~**Determine** the need for encryption technologies where sensitive data transmissions occur~~

~~**Consider** security issues of the remote / dial-up facilities and the need to **protect** these facilities from unauthorized use~~

~~**Review** and **recommend** changes to the system's Disaster Recovery Plan, Contingency Plan, Continuity of Operations Plan and System Security Plan~~

~~**Advise** SM on identifying controlled areas~~

~~**Make sure** necessary physical security is in place to protect system assets~~

~~**Authorize** movement of equipment into or out of controlled areas~~

~~**Develop** escort procedures to allow non-cleared individuals, including contract maintenance personnel, access to controlled areas~~

Appendix B – SLC Security Checklists

System Design Life Cycle Checklist: Vision Phase

This form represents the completion of all security related activities for the Vision Phase. The diagram below represents the deliverables completed during the development of *enter system name*.

Check if Complete	Name of Deliverable	Date Complete
☐	Business Case	
☐	RFP Security Requirements	
☐	Task Order Security Components	
☐	List of Business Partners	
☐	Assignment Letters	
☐	Security Artifact file system	
☐	Electronic Security Artifact File System	

Insert additional comments here:

SSO Name: enter SSO name

Signature: _____

Date: _____

SM Name: enter SM name

Signature: _____

Date: _____

System Design Life Cycle Checklist: Definition Phase

This form represents the completion of all security related activities for the Definition Phase. The diagram below represents the deliverables completed during the development of *enter system name*.

Check if Complete	Name of Deliverable	Date Complete
☐	System Roles and Responsibilities	
☐	~~System Identification and Analysis~~	
☐	~~Threat and Vulnerability Assessment~~	
☐	~~Security Guidance Compliance Matrix~~	
☐	~~GSS/MA Inventory Form~~	
☐	Interconnected System'(s) Security Documentation	
☐	MOU/SLA Draft	
☐	C&A Project Plan	
☐	System Rules of Behavior	
☐	Constructed clearance requirement matrix	
☐	Approved contractor access request form	

Insert additional comments here:

SSO Name: enter SSO name

Signature: _____

Date: _____

SM Name: enter SM name

Signature: _____

Date: _____

System Design Life Cycle Checklist: Construction Phase

This form represents the completion of all security related activities for the Construction Phase. The diagram below represents the deliverables completed during the development of *enter system name*.

Check if Complete	Name of Deliverable	Date Complete
☐	Draft System Security Plan	
☐	Draft Continuity of Operation Plan	
☐	Draft Disaster Recovery Plan	
☐	Draft System Security Authorization Agreement	
☐	Risk Assessment Report	
☐	~~Threat Analysis~~	
☐	~~Impact Analysis~~	
☐	Risk Assessment Corrective Action Plan	
☐	Cost Benefit Analysis	
☐	Final MOU/SLA	
☐	Completed User Background Investigation Clearance Form	
☐	Approved User Access Request Form	
☐	System Access Letters to Contractor Employees	

Insert additional comments here:

SSO Name: enter SSO name **Date:** _____

Signature: _____

SM Name: enter SSO name

Date: _____

Signature: _____

System Design Life Cycle Checklist: Deployment Phase

This form represents the completion of all security related activities for the Deployment Phase. The diagram below represents the deliverables completed during the development of *enter system name*.

Check if Complete	Name of Deliverable	Date Complete
☐	Documented Completion of CAP from Construction phase	
☐	Security Test Plan	
☐	Test Results	
☐	Final SSAA	
☐	Certification Letter	
☐	Signed Accreditation Letter	
☐	Final System Security Plan	
☐	Final Continuity of Operation Plan	
☐	Final Disaster Recovery Plan	
☐	User Training Schedule	
☐	Approved User Access Request Forms	

Insert additional comments here:

SSO Name: enter SSO name

Signature: _____

Date: _____

SM Name: enter SM name

Signature: _____

Date: _____

System Design Life Cycle Checklist: Support Phase

This form represents the completion of all security related activities for the Support Phase. The diagram below represents the deliverables completed during the development of *enter system name*.

Check if Complete	Name of Deliverable	Date Complete
☐	Re-certified and accredited SSAA	
☐	Documented completion of test results	
☐	Updated Operational Procedures	
☐	Updated Testing Results	

Insert additional comments here:

SSO Name: enter SSO name

Signature: _____

Date: _____

SM Name: enter SM name

Signature: _____

Date: _____

System Design Life Cycle Checklist: Retirement Phase

This form represents the completion of all security related activities for the Retirement Phase. The diagram below represents the deliverables completed during the development of *enter system name*.

Check if Complete	Name of Deliverable	Date Complete
☐	System Retirement Complete	

Insert additional comments here:

SSO Name: enter SSO name

Signature: _____

Date: _____

SM Name: enter SM name

Signature: _____

Date: _____

Appendix C - Assignment Letters

EXAMPLE System Manager Assignment Letter

MEMORANDUM

Month Day, Year

To: <System Manager>
<Title>

From: <Functional Manager>
<Title>

Subject: Formal Appointment of System Manager
<System Name>

This formally documents the appointment, effective immediately, of <System Manager> as the System Manager for the <System Name>. The System Manager is responsible for all actions related to the development, maintenance, and security of the <System Name>. They will provide advice to the Functional Manager on related matters and complete System Manager duties as described in ~~SFA~~FSA and Education policy, manuals, and guides.

cc: <~~SFA~~FSA/OCIO>

EXAMPLE System Security Officer

MEMORANDUM

Month Day, Year

To: <Functional Manager>
<Title>

From: <System Manager>
<Title>

Subject: Formal Appointment of System Security Officer
<System Name>

This formally documents the appointment, effective immediately, of the following individual(s) to the functions of System Security Officer (SSO) for the <System Name>. The SSO is responsible for implementation of security procedures directed by ~~SFA~~FSA, Education, and Federal Security Policy. They will provide advice to the System Manager on security related matters and complete SSO duties as described in ~~SFA~~FSA and Education policy, manuals, and guides. They will also participate as a member of the ~~SFA~~FSA Security Team led by the ~~SFA~~FSA Computer Security Officer.

Individual	Function
SSO's full name	SSO
Alternate SSO's full name	Alt-SSO (if applicable)

cc: <Computer Security Officer (Andy Boots)>

Appendix D – Security SLC Project Plan